(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－99403
（P2000－99403A）
(43)公開日　平成12年４月７日(2000.4.7)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
	３１０		３１０Ｋ	

審査請求　未請求　請求項の数26　ＯＬ　（全 11 頁）

(21)出願番号　特願平10－265210

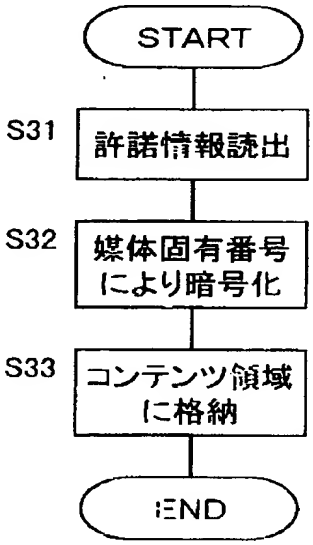
(22)出願日　平成10年９月18日(1998.9.18)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　小谷　誠剛
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　長谷部　高行
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100094145
弁理士　小野　由己男　（外２名）

最終頁に続く

(54)【発明の名称】　情報管理方法および情報管理装置

(57)【要約】
【課題】　記録媒体上に格納された電子化データを利用するために必要な許諾情報がなんらかの障害により破壊された場合であっても、ユーザがバックアップ情報を用いてこれを復帰させることが可能な情報管理方法を提供する。
【解決手段】　記録媒体のユーザによるアクセスが不可能な第２階層に格納されている許諾情報を読み出して（ステップＳ３１）、記録媒体の媒体固有番号によって暗号化し（ステップＳ３２）、暗号化した許諾情報を記録媒体のユーザが任意に利用できる第３階層に格納する（ステップＳ３３）。



【特許請求の範囲】

【請求項１】媒体固有の情報を有する記録媒体上の所定の領域に格納された所定の情報を、前記媒体固有の情報またはそれに基づいて生成された鍵により暗号化して前記所定の領域外に導出する情報管理方法。

【請求項２】前記記録媒体は、前記所定の情報を格納する第１領域と、前記第１領域と異なる第２領域とを備える、請求項１に記載の情報管理方法。

【請求項３】前記第２領域は外部からの指令に基づいて任意の情報を書込・読出可能なユーザ利用領域であり、前記第１領域は外部からの指令に基づいて制御することが不可能な機密領域である、請求項２に記載の情報管理方法。

【請求項４】前記第２領域に格納される任意の情報は暗号化された電子化データであり、前記第１領域に格納される所定の情報は前記電子化データを利用する利用権に基づく許諾情報を含む、請求項３に記載の情報管理方法。

【請求項５】前記所定の情報は、前記媒体固有の情報またはそれに基づいて生成された鍵により暗号化されて前記所定の領域に格納されている、請求項２～４のいずれかに記載の情報管理方法。

【請求項６】前記所定の情報は、前記記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵により暗号化されている、請求項５に記載の情報管理方法。

【請求項７】前記暗号化された所定の情報を前記第２領域に格納する、請求項２～６のいずれかに記載の情報管理方法。

【請求項８】前記第２領域に格納されている暗号化された所定の情報を前記媒体固有の情報またはそれに基づいて生成された鍵により復号化し、前記第１領域に格納されている所定の情報を更新する、請求項７に記載の情報管理方法。

【請求項９】前記所定の情報を前記第１領域外に導出する際に、前記媒体固有の情報またはそれに基づいて生成された鍵および前記記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵により暗号化する、請求項７に記載の情報管理方法。

【請求項１０】前記第２領域に格納されている暗号化された所定の情報を、前記記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵および前記媒体固有の情報またはそれに基づいて生成された鍵により復号化して、前記第１領域に格納されている所定の情報を更新する、請求項９に記載の情報管理方法。

【請求項１１】前記暗号化された所定の情報を、前記記録媒体とは異なる第２の記録媒体上に格納する、請求項１～６のずれかに記載の情報管理方法。

【請求項１２】前記第２の記録媒体に格納されている暗号化された所定の情報を前記媒体固有の情報またはそれに基づいて生成された鍵により復号化し、前記所定の領域に格納されている所定の情報を更新する、請求項１１に記載の情報管理方法。

【請求項１３】前記所定の情報を前記第２の記録媒体上に導出する際に、前記媒体固有の情報またはそれに基づいて生成された鍵および前記第２の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵により暗号化する、請求項１１に記載の情報管理方法。

【請求項１４】前記第２の記録媒体に格納されている暗号化された所定の情報を、前記第２の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵および前記媒体固有の情報またはそれに基づいて生成された鍵により復号化して、前記所定の領域に格納されている所定の情報を更新する、請求項１３に記載の情報管理方法。

【請求項１５】前記媒体固有の情報は前記記録媒体から電子的に入手できるとともに可視的に前記記録媒体上に表示されている、請求項１～１４にいずれかに記載の情報管理方法。

【請求項１６】前記記録媒体を駆動する装置に固有の情報は、前記装置から電子的に入手できるとともに可視的に前記装置上に表示されている、請求項６、９または１０に記載の情報管理方法。

【請求項１７】前記第２の記録媒体を駆動する装置に固有の情報は、前記装置から電子的に入手できるとともに可視的に前記装置上に表示されている、請求項１３または１４に記載の情報管理方法。

【請求項１８】媒体固有の情報を有し、外部からの指令に基づいて任意の情報を書込・読出可能なユーザ利用領域と、外部からの指令に基づいて制御することが不可能な機密領域とを備え、前記ユーザ利用領域に格納された任意の情報に対する利用権に基づく許諾情報が前記機密領域に格納されている記録媒体の情報を管理する情報管理装置であって、

前記ユーザ利用領域に対して任意の情報を書込・読出を行う書込・読出手段と、

前記機密領域に格納されている許諾情報を前記媒体固有の情報またはそれに基づいて生成された鍵により暗号化して前記機密領域外に導出する所定情報導出手段と、を備える情報管理装置。

【請求項１９】前記暗号化された許諾情報を、前記書込・読出手段により前記ユーザ利用領域に格納する、請求項１８に記載の情報管理装置。

【請求項２０】前記ユーザ利用領域に格納されている暗号化された許諾情報を前記媒体固有の情報により復号化して前記機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える、請求項１９に記載の情報管理装置。

【請求項２１】装置固有の情報を備え、前記所定情報導出手段は、前記許諾情報を前記媒体固有の情報またはそ

れに基づいて生成された鍵および前記装置に固有の情報またはそれに基づいて生成された鍵により暗号化する、請求項１８または１９に記載の情報管理装置。

【請求項２２】前記ユーザ利用領域に格納されている暗号化された許諾情報を前記装置に固有の情報またはそれに基づいて生成された鍵および前記媒体固有の情報またはそれに基づいて生成された鍵により復号化して前記機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える、請求項２１に記載の情報管理装置。

【請求項２３】前記所定情報導出手段は、前記暗号化された許諾情報を前記記録媒体とは異なる第２の記録媒体に送出する、請求項１８に記載の情報管理装置。

【請求項２４】前記第２の記録媒体に格納されている暗号化された許諾情報を前記媒体固有の情報により復号化して前記機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える、請求項２３に記載の情報管理装置。

【請求項２５】前記第２の記録媒体を駆動する装置は装置固有の情報を備え、前記所定情報導出手段は、前記許諾情報を前記媒体固有の情報またはそれに基づいて生成された鍵および前記第２の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵により暗号化する、請求項２３に記載の情報管理装置。

【請求項２６】前記第２の記録媒体に格納されている暗号化された許諾情報を、前記第２の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵および前記媒体固有の情報またはそれに基づいて生成された鍵により復号化して前記機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える、請求項２５に記載の情報管理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報管理方法および情報管理装置に関し、特に、媒体固有の情報を有する記録媒体に対して任意の情報を記録・読出を行う際の情報管理方法およびその装置に関する。

【０００２】

【従来の技術】コンピュータプログラムなどのソフトウェアや電子出版物では、光磁気ディスク（ＭＯ）、ディジタルビデオディスク（ＤＶＤ）、フロッピーディスク（ＦＤ）、ミニディスク（ＭＤ）、その他の記録媒体上に電子化データを格納して販売される。このような電子化データは、一般にコピーが容易であり、不正コピーが頻繁に行われている。このため、ソフトウェアベンダーや出版者側の著作権が侵害され著しく利益が阻害されるおそれがある。

【０００３】このような記録媒体上に格納された電子化データを保護するために、ユーザ固有の情報を用いて暗号化した許諾情報を生成し、これを記録媒体上の所定の領域に格納して配布することが提案されている。ソフトウェアや出版物などの電子化データは、所定の暗号鍵によって暗号化されて記録媒体上に格納されている。また、この暗号化された電子化データを復号化するための復号鍵がユーザ固有の情報を用いて暗号化され、許諾情報として記録媒体上に格納されている。

【０００４】ユーザ側では、この許諾情報をユーザ固有の情報により復号化することによって復号鍵を得ることができ、記録媒体上に格納されている暗号化された電子化データをこの復号鍵を用いて復号化して利用することができる。このように構成することによって、ユーザ個々に電子化データの利用権を与える際に、電子化データを暗号化するための暗号鍵を共通にすることができ、ユーザ毎に異なるユーザ固有の情報を用いて復号鍵を暗号化することによって、利用権を個々に与えることが可能となる。

【０００５】ここで用いられるユーザ固有の情報とは、例えば、ユーザが使用しているコンピュータまたは記録媒体を駆動する装置に付与されている装置番号である。したがって、ユーザが正規に入手したものであっても、異なる装置では使用できなくなり、この記録媒体を譲渡することもできないという不都合がある。特開平5-257816号公報には、記録媒体にこの媒体固有の情報を与え、暗号化された電子化データを復号するための復号鍵をこの媒体固有の情報により暗号化して記録媒体に格納するようにした方法が提案されている。

【０００６】この場合、前述の場合と同様に、電子化データを暗号化する際の暗号鍵を共通にすることができ、ユーザ毎に異なる媒体固有の情報を用いて復号鍵を暗号化することによって、利用権を個々に与えることが可能となる。

【０００７】

【発明が解決しようとする課題】上述のような方法においては、暗号化された電子化データは、ユーザがアクセス可能な領域に格納される。また、この電子化データを利用するための許諾情報は、ユーザがアクセス不可能な機密領域に格納される。したがって、正規のユーザであっても許諾情報を読み出してバックアップをとることができず、この機密領域に格納されているデータがなんらかの障害により破壊された場合には、電子化データを利用することができなくなる。このような場合には、ソフトウェアベンダーや出版者、その代理店などの電子化データの管理者による利用権の再発行が必要となる。したがって、この再発行の手続きに煩雑な作業と余分なコストを必要とすることとなる。

【０００８】本発明は、記録媒体上に格納された電子化データを利用するために必要な許諾情報がなんらかの障害により破壊された場合であっても、ユーザがバックアップ情報を用いてこれを復帰させることが可能な情報管理方法および情報管理装置を提供することを目的とす

る。

【0009】

【課題を解決するための手段】本発明に係る情報管理方法は、媒体固有の情報を有する記録媒体上の所定の領域に格納された所定の情報を、媒体固有の情報またはそれに基づいて生成された鍵により暗号化して所定の領域外に導出する。ここで、記録媒体は、所定の情報を格納する第１領域と、第１領域と異なる第２領域とを備える構成とすることができる。

【0010】また、第２領域は外部からの指令に基づいて任意の情報を書込・読出可能なユーザ利用領域であり、第１領域は外部からの指令に基づいて制御することが不可能な機密領域で構成することができる。この場合、第２領域に格納される任意の情報は暗号化された電子化データであり、第１領域に格納される所定の情報は電子化データを利用する利用権に基づく許諾情報を含むように構成できる。

【0011】また、所定の情報は、媒体固有の情報またはそれに基づいて生成された鍵により暗号化されて所定の領域に格納される構成とすることができる。さらに、所定の情報は、記録媒体を駆動する装置に固有の情報に基づいて暗号化される構成であってもよい。また、暗号化された所定の情報を第２領域に格納する構成とすることができる。

【0012】この場合、第２領域に格納されている暗号化された所定の情報を媒体固有の情報またはそれに基づいて生成された鍵により復号化し、第１領域に格納されている所定の情報を更新するように構成できる。また、所定の情報を第１領域外に導出する際に、媒体固有の情報またはそれに基づいて生成された鍵および記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵により暗号化するように構成できる。

【0013】この場合には、第２領域に格納されている暗号化された所定の情報を、記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵および媒体固有の情報またはそれに基づいて生成された鍵により復号化して、第１領域に格納されている所定の情報を更新するように構成できる。上述のような構成とすることによって、所定の情報を格納されている所定の領域外に導出する場合には、この媒体に固有の情報により暗号化されているので、他の記録媒体にコピーしても、これを復号化することが困難である。例えば、第２領域にソフトウェアや出版物などの電子化データを格納する際に、この電子化データを暗号鍵により暗号化して格納しておき、これを復号するための復号鍵をこの記録媒体に固有の情報で暗号化してユーザのアクセス不可能な第１領域に格納しておけば、暗号化するための暗号鍵をユーザ個々に変える必要がなく、共通の暗号鍵を用いて暗号化して格納できる。第１領域に格納されている暗号化された復号鍵は、さらに媒体固有の情報を用いて暗号化されて、第１領域外に導出するように構成しているため、ユーザのバックアップとして保存しておくことが可能である。この保存されたバックアップデータは、媒体固有の情報により暗号化されているため、これを他の記録媒体にコピーしても復号化することが困難であり、電子化データを復号するための復号鍵を得ることは困難である。

【0014】また、所定の領域に格納されている情報が破壊されてもこのバックアップデータに基づいてユーザ側で許諾情報を復元することが可能であり、煩わしい利用権の再発行の手続きを必要としない。また、暗号化された所定の情報を、記録媒体とは異なる第２の記録媒体上に格納するように構成できる。

【0015】この場合、第２の記録媒体に格納されている暗号化された所定の情報を媒体固有の情報またはそれに基づいて生成された鍵により復号化し、所定の領域に格納されている所定の情報を更新するように構成できる。また、所定の情報を第２の記録媒体上に導出する際に、媒体固有の情報またはそれに基づいて生成された鍵および第２の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵により暗号化するように構成できる。

【0016】この場合には、第２の記録媒体に格納されている暗号化された所定の情報を、第２の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵および媒体固有の情報またはそれに基づいて生成された鍵により復号化して、所定の領域に格納されている所定の情報を更新するように構成できる。また、媒体固有の情報は記録媒体から電子的に入手できるとともに可視的に記録媒体上に表示されていることが好ましく、記録媒体を駆動する装置に固有の情報および第２の記録媒体を駆動する装置に固有の情報は、装置から電子的に入手できるとともに可視的に装置上に表示されていることが好ましい。

【0017】この場合には、前述したような許諾情報のバックアップデータを第２の記録媒体に保存しておき、第１領域に格納されたデータが破壊されたときに、この第２の記録媒体に格納された情報に基づいて、これを復元することが可能となる。本発明に係る情報管理装置は、媒体固有の情報を有し、外部からの指令に基づいて任意の情報を書込・読出可能なユーザ利用領域と、外部からの指令に基づいて制御することが不可能な機密領域とを備え、ユーザ利用領域に格納された任意の情報に対する利用権に基づく許諾情報が機密領域に格納されている記録媒体の情報を管理する情報管理装置であって、ユーザ利用領域に対して任意の情報を書込・読出を行う書込・読出手段と、機密領域に格納されている許諾情報を媒体固有の情報またはそれに基づいて生成された鍵により暗号化して機密領域外に導出する所定情報導出手段とを備えている。

【0018】ここで、暗号化された許諾情報を、書込・

読出手段によりユーザ利用領域に格納する構成とすることができる。また、ユーザ利用領域に格納されている暗号化された許諾情報を媒体固有の情報により復号化して機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える構成とすることができる。

【００１９】さらに、装置固有の情報を備え、所定情報導出手段は、許諾情報を媒体固有の情報またはそれに基づいて生成された鍵および装置に固有の情報またはそれに基づいて生成された鍵により暗号化するように構成できる。この場合、ユーザ利用領域に格納されている暗号化された許諾情報を装置に固有の情報またはそれに基づいて生成された鍵および媒体固有の情報により復号化して機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える構成とすることができる。

【００２０】また、所定情報導出手段は、暗号化された許諾情報を記録媒体とは異なる第２の記録媒体に送出するように構成できる。この場合、第２の記録媒体に格納されている暗号化された許諾情報を媒体固有の情報により復号化して機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える構成とすることができる。

【００２１】また、第２の記録媒体を駆動する装置は装置固有の情報を備え、所定情報導出手段は、許諾情報を媒体固有の情報またはそれに基づいて生成された鍵および第２の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵により暗号化するように構成できる。この場合には、第２の記録媒体に格納されている暗号化された許諾情報を、第２の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵および媒体固有の情報により復号化して機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える構成とすることができる。

【００２２】

【発明の実施の形態】本発明の実施形態について図面を参照して説明する。

〔記録媒体〕本発明に用いられる記録媒体は、光磁気ディスク（ＭＯ）、ディジタルビデオディスク（ＤＶＤ）、フロッピーディスク（ＦＤ）、ミニディスク（ＭＤ）、その他のユーザによるデータの書き換えが可能な記録媒体であり、例えば光磁気ディスクについてその記録領域を図１により説明する。

【００２３】記録媒体１は、ユーザによる読み出しは可能であるが書き換えが不可能な第１階層２、外部からの指令による読み出し・書き込みが不可能な第２階層３、ユーザが任意に情報の書き込みを行うことが可能な第３階層４を有している。第１階層２には、その媒体について一意に決定される媒体固有番号２が格納されている。第３階層４は、ユーザが任意の情報７を格納することが可能な領域であり、ユーザが利用するためのコンピュータプログラム、電子出版物、その他任意のデータを格納するユーザコンテンツ領域である。第２階層３は、第３階層４に格納された任意の情報に基づく所定の情報６を格納するための領域であり、たとえば、第３階層４に格納されているコンピュータプログラムや電子出版物などの利用権に基づく許諾情報などが格納される。

〔許諾側の構成〕記録媒体に電子化データを格納して配布する際に、この電子化データを利用するための利用権をユーザ毎に設定する場合、この電子化データを暗号化して記録媒体に格納する。　たとえば、図２に示すように、記録媒体１１に電子化データを格納する場合、第１階層１２に媒体固有番号１５、第２階層１３に利用権に基づく許諾情報１６、第３階層１４に暗号化されたコンテンツ１７が格納される。ここで、許諾情報１６は、ユーザの利用権に基づくデータであり、たとえば暗号化されたコンテンツ１７を復号化するための復号鍵とすることができる。

【００２４】許諾側のコンピュータ２１では、個別鍵生成手段２２、許諾情報暗号化手段２３、コンテンツ暗号化手段２４、暗号鍵テーブル２５、復号鍵テーブル２６などを備えている。コンテンツ暗号化手段２４は、暗号鍵テーブル２５の暗号鍵によりコンテンツとなるデータ２７を暗号化し、記録媒体１１の第３階層１４にコンテンツとして格納する。暗号鍵テーブル２５の暗号鍵に対応する復号鍵が復号鍵テーブル２６に格納される。個別鍵生成手段２２は、記録媒体１１の第１階層１２から読み出した媒体固有番号１５をもとに媒体個別鍵を生成する。許諾情報暗号化手段２３は、復号鍵テーブル２６の復号鍵を媒体個別鍵により暗号化して、記録媒体１１の第２階層１３に許諾情報１６として格納する。

〔ユーザ側の構成〕図１の記録媒体１を駆動するためのユーザ側の駆動装置を図４にその概念構成図として示す。

【００２５】駆動装置３１は、ユーザ利用領域である第３階層４に任意の情報７の書き込み、読み出しを行う書込・読出手段３２と、機密領域である第２階層３に格納されている所定の情報６を第１階層２に格納されている媒体固有番号５を用いて暗号化し第２階層３以外の領域に導出する所定情報導出手段３３とを備えている。所定情報導出手段３３が許諾情報などの所定の情報を暗号化して導出する場所としては、たとえば、第３階層４または他の記録媒体が考えられる。暗号化した許諾情報を記録媒体１の第３階層４に格納する場合には、書込・読出手段３２により任意の情報７として格納させることができる。

【００２６】さらに具体的な構成の一例として図４に簡略ブロック図を示す。ユーザ側の駆動装置４１は、個別鍵生成手段４２、許諾情報復号化手段４３、復号鍵格納部４４、コンテンツ復号化手段４５、復号データ格納部４６、許諾情報暗号化手段４７などを備えている。個別鍵生成手段４２は、記録媒体１１の第１階層１２に格納

されている媒体固有番号１５に基づいて媒体個別鍵を生成するものであって、許諾側の個別鍵生成手段２２によって生成される個別鍵と同じものを生成する。許諾情報復号化手段４３は、記録媒体１１の第２階層１３に格納されている許諾情報１６を読み出して、個別鍵生成手段４２により生成された個別鍵により復号化する。許諾情報復号化手段４３によって復号化された許諾情報は、復号鍵格納部４４に一時的に格納される。コンテンツ復号化手段４５は、記録媒体１１の第３階層１４に格納されているコンテンツ１７を読み出して、復号鍵格納部４４に格納されている復号鍵を用いて復号化し、復号データ格納部４６に格納するものである。

【００２７】許諾情報暗号化手段４７は、第２階層１３の許諾情報１６を読み出して、第１階層１２に格納されている媒体固有番号１２を用いて暗号化する。この場合、媒体固有番号１２をそのまま用いることも可能であり、個別鍵生成手段４２によって生成した個別鍵を用いて暗号化することも可能であり、さらに、媒体固有番号１２に基づいて暗号鍵を生成しこれを用いて暗号化することも可能である。このあと、暗号化した許諾情報を記録媒体１１の第３階層１４内に格納する。

〔コンテンツ格納処理〕許諾側において記録媒体１１に電子化データを格納する際の動作を図５にフローチャートとして示す。

【００２８】ステップＳ１では、記録媒体１１に格納するコンピュータプログラム、電子出版物、その他の電子化データの作成を行う。ステップＳ２では、電子化データを暗号化するための暗号鍵の作成を行う。ステップＳ３では、暗号化を行う電子化データと暗号鍵とを対応させて、暗号鍵テーブル２５に格納する。このとき同時に、暗号鍵により暗号化されたデータを復号するための復号鍵が作成され、電子化データと復号鍵とを対応させて復号鍵テーブル２６に格納する。暗号鍵と復号鍵とを共通のものとし、暗号鍵テーブル２５と復号鍵テーブル２６とを１つの鍵管理テーブルとすることも可能である。

【００２９】ステップＳ４では、暗号化を行う電子化データに対応する暗号鍵を暗号鍵テーブル２５から取り出す。ステップＳ５では、電子化データを暗号鍵により暗号化する。たとえば、ＤＥＳ暗号を用いる場合には、暗号化を行う電子化データに対して換字とビット転置を繰り返して暗号化を行う。ステップＳ６では、暗号化された電子化データをコンテンツ１７として、記録媒体１１の第３階層１４に格納する。ステップＳ７では、暗号化された電子化データの格納が終了したか否かを判別する。暗号化された電子化データの格納がすべて終了した場合には、ステップＳ８に移行する。

【００３０】ステップＳ８では、記録媒体１１の第１階層１２から媒体固有番号１５を読み出して個別鍵を生成する。ステップＳ９では、コンテンツ１７として記録媒体１１に格納した電子化データに対応する復号鍵を復号鍵テーブル２６から読み出して、ステップＳ８で生成した個別鍵により暗号化する。コンテンツ１７として格納した電子化データに対応する復号鍵をすべて暗号化した後、ステップＳ１０において、この暗号化した復号鍵を許諾情報１６とし記録媒体１１の第２階層１３に格納する。

〔電子化データの復号化処理〕記録媒体１１の第３階層１４に格納されているコンテンツ１７は、許諾側が作成した暗号鍵によって暗号化されているため、ユーザ側でこれを利用するためには適切な復号鍵により復号化する必要がある。このときの動作を図６のフローチャートを用いて説明する。　記録媒体１１が駆動装置４１に装着されてデータのロード命令がなされると、ステップＳ２１において、記録媒体１１の第１階層１２から媒体固有番号１５を読み出す。ステップＳ２２では、媒体固有番号１５から個別鍵の生成を行う。ここでは、許諾側のステップＳ８と同じアルゴリズムにより個別鍵を生成する。ステップＳ２３では、記録媒体１１の第２階層１３に格納されている許諾情報１６を読み出してこれをステップＳ２２で生成した個別鍵を用いて復号化する。ここで復号化された許諾情報は、コンテンツ１７を復号化するための復号鍵であり、この復号鍵を第３領域１４に格納されている電子化データと対応させて復号鍵テーブルとし、これを復号鍵格納部４４に一時的に格納する。

【００３１】ステップＳ２４では、記録媒体１１の第３階層１４に格納されているコンテンツ１７を読み込む。ステップＳ２５では、復号鍵格納部４４に格納されている復号鍵を用いて、読み込んだコンテンツ１７を復号化する。ステップＳ２６では、復号化されたコンテンツを実行する。

〔許諾情報のバックアップ処理〕ユーザ側の駆動装置４１において、記録媒体１１の第２階層１３に格納されている許諾情報１６はバックアップデータとして保存される。この処理を図７を用いて説明する。

【００３２】ステップＳ３１では、記録媒体１１の第２階層１３に格納されている許諾情報１６を読み出す。ステップＳ３２では、読み出した許諾情報１６を媒体固有番号１５によって暗号化する。このとき、ステップ２２により生成された個別鍵を用いて許諾情報１６の暗号化を行うことも可能であり、他のアルゴリズムにより媒体固有番号１５を暗号化した鍵を用いて暗号化するように構成することも可能である。ステップＳ３３では、暗号化された許諾情報１６を記録媒体１１の第３階層１４内に格納する。

【００３３】このような構成の場合、第３階層１４内に許諾情報１６のバックアップが保存されているため、第２階層１３の許諾情報１６が破壊されたときに、第３階層１４内のバックアップデータを読み出して第２階層１３に戻せば、許諾情報１６の再発行を待たずにコンテン

ツ１７を利用することが可能となる。また、第３階層１４に保存されている許諾情報は、媒体固有番号１５によって暗号化されているため、記録媒体１１の第３階層１４に格納されている内容がそっくりコピーされても、元の許諾情報１６を復元することは困難であり、コンテンツ１７の不正利用を防止することができる。

〔他の実施形態〕

（Ａ）記録媒体１１の第２階層１３に格納されている許諾情報１６が破壊された場合に、第３階層１４に保存しておいた許諾情報のバックアップデータを用いて許諾情報１６を復元する機能が、記録媒体１１を駆動する駆動装置に備わっている場合について説明する。　図８は、このような駆動装置５１の制御ブロック図であり、個別鍵生成手段４２、許諾情報復号化手段４３、復号鍵格納部４４、コンテンツ復号化手段４５、復号データ格納部４６および許諾情報暗号化手段４７は、図４に示した実施形態と同様であり説明を省略する。

【００３４】許諾情報更新手段５２は、記録媒体１１の第３階層１４に保存されている暗号化された許諾情報を読み出して、これを第１階層１２に格納されている媒体固有番号１５によって復号化する。ここで、第３階層１４に保存されている許諾情報が個別鍵生成手段４２によって生成された個別鍵により暗号化されている場合には、復号化に用いる鍵はこの個別鍵を用いることとなる。このあと、復号化された許諾情報は、許諾情報１６として記録媒体１１の第２階層１３に格納される。

【００３５】この実施形態の動作について図９にフローチャートとして示す。ステップＳ４１では、記録媒体１１の第３階層１４に格納されている暗号化された許諾情報を読み出す。ステップＳ４２では、読み出した暗号化された許諾情報を媒体固有番号１５によって復号化する。このとき、ステップ２２により生成された個別鍵を用いて許諾情報の復号化を行うことも可能であり、他のアルゴリズムにより媒体固有番号１５を暗号化した鍵を用いて暗号化されている場合には、この鍵を用いて復号化を行う。ステップＳ４３では、復号化された許諾情報を記録媒体１１の第２階層１３に許諾情報１６として格納する。

【００３６】このことにより、記録媒体１１の第２階層１３に格納されている許諾情報１６はなんらかの障害により破壊された場合には、第３階層１４にバックアップデータとして保存されている暗号化された許諾情報を用いて復元することが可能である。この復元処理は、駆動装置５１内で処理されるため、許諾情報１６が外部に出力されることがなく、この情報を不正に利用することは不可能となっている。

（Ｂ）記録媒体１１を駆動するための駆動装置に固有の装置固有番号によりさらに暗号化を行う場合の実施形態を図１０～図１２に示す。

【００３７】図１０に示すように、駆動装置６１において、個別鍵生成手段４２、許諾情報復号化手段４３、復号鍵格納部４４、コンテンツ復号化手段４５、復号データ格納部４６および許諾情報暗号化手段４７は、図４に示した実施形態と同様であり説明を省略する。また、駆動装置６１は装置固有番号を格納する装置固有番号格納部６２を備えている。さらに、第２許諾情報暗号化手段６３を備えている。この第２許諾情報暗号化手段６３は、許諾情報暗号化手段４７で媒体固有番号１５によって暗号化された許諾情報を、さらに装置固有番号によって暗号化するものである。この第２許諾情報暗号化手段６３によって暗号化された許諾情報は、記録媒体１１の第３階層１４内に格納される。

【００３８】また、駆動装置６１は許諾情報更新手段６４を備えている。この許諾情報更新手段６４は、記録媒体１１の第３階層１４に保存されている暗号化された許諾情報を読み出して、これを装置固有番号格納部６２に格納されている装置固有番号により復号化する第１許諾情報復元手段６５と、第１許諾情報復元手段６５が復号化した許諾情報を記録媒体１１の第１階層１２に格納されている媒体固有番号１５によって復号化する第２許諾情報復元手段６６とを備えている。復元された許諾情報は、記録媒体１１の許諾情報１６として第２階層１３に格納される。

【００３９】記録媒体１１に格納されている許諾情報１６のバックアップを保存する際には、図１１に示す手順で行われる。まず、ステップＳ５１では、記録媒体１１の第２階層１３に格納されている許諾情報１６を読み出す。ステップＳ５２では、読み出した許諾情報１６を第１階層１２に格納されている媒体固有番号１５によって暗号化する。ステップＳ５３では、媒体固有番号１５によって暗号化された許諾情報を、装置固有番号格納部６２に格納された装置固有番号により暗号化する。このあと、暗号化された許諾情報をステップＳ５４において第３階層１４内に格納する。

【００４０】記録媒体１１に格納されている許諾情報１６が破壊された場合には、図１２に示す手順で許諾情報の復元を行う。ステップＳ６１では、記録媒体１１の第３階層１４に格納されている暗号化された許諾情報を読み出す。ステップＳ６２では、読み出した暗号化された許諾情報を装置固有番号により復号化する。ステップＳ６３では、装置固有番号により復号化された許諾情報を媒体固有番号１５によって復号化する。ステップＳ６４では、復号化された許諾情報を記録媒体１１の第２階層１３に許諾情報１６として格納する。

【００４１】このように構成した場合には、許諾情報１６のバックアップデータが媒体固有番号１５によって暗号化され、さらに駆動装置６１の装置固有番号によって暗号化されているため、データの違法コピーを行っても利用することができず、著作権保護をすることができる。また、記録媒体１１の許諾情報１６が破壊されたと

しても、この駆動装置６１を用いて復元することが可能であり、正規のユーザであれば再発行を待たずにコンテンツの利用が可能となる。

【００４２】装置固有番号は、記録媒体１１を駆動するための駆動装置６１に固有の装置番号としたが、ユーザ側で使用しているコンピュータに固有の装置番号を利用することも可能である。また、許諾情報１６のバックアップデータを保存する際に装置固有番号によって暗号化した後、媒体固有番号１５によって暗号化して格納することも可能であり、これを復元する場合は媒体固有番号１５によって復号化した後に装置固有番号によって復号化することとなる。

（Ｃ）許諾情報１６のバックアップデータを他の記録媒体に保存しておくことも可能である。このような実施形態について、図１３～図１５に基づいて説明する。

【００４３】記録媒体１１を駆動するための駆動装置７１は、第２の記録媒体８３を駆動するための駆動装置８１と接続されており、媒体間のデータのやりとりが可能となっている。駆動装置８１は、たとえば、フロッピーディスクドライブ（ＦＤＤ）、ハードディスクドライブ（ＨＤＤ）、ミニディスク（ＭＤ）、光磁気ディスク（ＭＯ）、デジタルディスクドライブ（ＤＶＤ）などが採用され、装置固有番号を格納するための装置固有番号格納部８２を備えており、この装置固有番号を電子データとして出力することが可能となっている。

【００４４】記録媒体１１を駆動する駆動装置７１において、個別鍵生成手段４２、許諾情報復号化手段４３、復号鍵格納部４４、コンテンツ復号化手段４５、復号データ格納部４６および許諾情報暗号化手段４７は、図４に示した実施形態と同様であり説明を省略する。駆動装置７１は、さらに、第２許諾情報暗号化手段７２と、許諾情報更新手段７３とを備えている。第２許諾情報暗号化手段７２は、許諾情報暗号化手段４７によって暗号化された許諾情報を、さらに駆動装置８１の装置固有番号によって暗号化する。このあと、暗号化された許諾情報を第２の記録媒体８３に格納する。

【００４５】許諾情報更新手段７３は、第２の記録媒体８３に保存されている暗号化された許諾情報を読み出して、これを装置固有番号格納部８２に格納されている装置固有番号により復号化する第１許諾情報復元手段７４と、第１許諾情報復元手段７４が復号化した許諾情報を記録媒体１１の第１階層１２に格納されている媒体固有番号１５によって復号化する第２許諾情報復元手段７５とを備えている。復元された許諾情報は、記録媒体１１の許諾情報１６として第２階層１３に格納される。

【００４６】記録媒体１１に格納されている許諾情報１６のバックアップを保存する際には、図１４に示す手順で行われる。まず、ステップＳ７１では、記録媒体１１の第２階層１３に格納されている許諾情報１６を読み出す。ステップＳ７２では、読み出した許諾情報１６を第１階層１２に格納されている媒体固有番号１５によって暗号化する。ステップＳ７３では、媒体固有番号１５によって暗号化された許諾情報を、第２の記録媒体８３を駆動するための駆動装置８１の装置固有番号により暗号化する。このあと、暗号化された許諾情報をステップＳ７４において第３階層１４内に格納する。

【００４７】記録媒体１１に格納されている許諾情報１６が破壊された場合には、図１５に示す手順で許諾情報１６の復元処理が行われる。ステップＳ８１では、第２の記録媒体８３に格納されている暗号化された許諾情報を読み出す。ステップＳ８２では、読み出した暗号化された許諾情報を第２の記録媒体８３を駆動する駆動装置８１の装置固有番号により復号化する。ステップＳ８３では、装置固有番号により復号化された許諾情報を媒体固有番号１５によって復号化する。ステップＳ８４では、復号化された許諾情報を記録媒体１１の第２階層１３に許諾情報１６として格納する。

【００４８】このように構成した場合には、許諾情報１６のバックアップデータを記録媒体１１と切り離して管理することができ、高いセキュリティを維持することができる。また、複数の記録媒体について、その許諾情報をユーザ側で管理することが可能であり、許諾情報がなんらかの形で破壊されても、ユーザ側で対応することが可能である。ここでも、許諾情報１６を暗号化する際に、装置固有番号で暗号化した後、媒体固有番号で暗号化するように構成してもよい。この場合には、これを復元する際には、媒体固有番号で復号化した後に装置固有番号で復号化することとなる。

（Ｄ）ケーブルテレビやインターネットなどにおいて暗号化したデータを放送し、これをユーザ側で記録媒体に記録させる場合に、上述のような方法を適用することができる。たとえば、ユーザ側から暗号化データを記録した記録媒体の媒体固有番号を放送局に送信させ、その媒体固有番号で暗号化された復号鍵をユーザに送信する。ユーザ側の装置では、この復号鍵を記録媒体の第２階層の許諾情報として格納する。さらに、この許諾情報を媒体固有番号によって暗号化して第３階層に格納する。

【００４９】記録媒体上のコンテンツを利用する場合には、媒体固有番号により許諾情報を復号化して復号鍵を生成し、暗号化されたデータを復号化すればよい。この場合にも、他の記録媒体にコンテンツをそのままコピーしても、許諾情報が媒体固有番号によって暗号化されており、復号化することが困難である。また、バックアップデータを用いて許諾情報を復元することが可能であり、許諾情報が破壊された場合であっても、ユーザ側で復元することが可能である。

【００５０】

【発明の効果】本発明によれば、記録媒体の所定の領域に格納された所定の情報を、媒体固有の情報によって暗号化して導出しており、他の記録媒体にコピーしても、

これを復号化することが困難である。例えば、ソフトウェアや出版物などの電子化データを格納する際に、この電子化データを暗号鍵により暗号化して格納しておき、これを復号するための復号鍵をこの記録媒体に固有の情報で暗号化してユーザのアクセス不可能な領域に格納しておけば、暗号化するための暗号鍵をユーザ個々に変える必要がなく、共通の暗号鍵を用いて暗号化して格納できる。暗号化された復号鍵は、さらに媒体固有の情報を用いて暗号化されて、所定の領域外に導出するように構成しているため、ユーザのバックアップとして保存しておくことが可能である。この保存されたバックアップデータは、媒体固有の情報により暗号化されているため、これを他の記録媒体にコピーしても復号化することが困難であり、電子化データを復号するための復号鍵を得ることは困難である。また、ユーザはこのバックアップデータを用いて復号鍵を復元することができるため、データがなんらかの障害が破壊された場合であっても、再発行の手続きを省略することが可能となる。

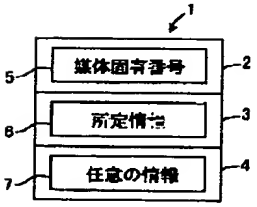
【図面の簡単な説明】

【図１】本発明に用いられる記録媒体の記録領域を示す概念図。
【図２】許諾側における簡略ブロック図。
【図３】本発明の概念構成図。
【図４】１実施形態の簡略ブロック図。
【図５】コンテンツ格納処理の制御フローチャート。
【図６】復号化処理の制御フローチャート。
【図７】バックアップ処理の制御フローチャート。
【図８】他の実施形態の簡略ブロック図。
【図９】許諾情報更新処理のフローチャート。
【図１０】他の実施形態の簡略ブロック図。
【図１１】その制御フローチャート。
【図１２】その制御フローチャート。
【図１３】他の実施形態の簡略ブロック図。
【図１４】その制御フローチャート。
【図１５】その制御フローチャート。

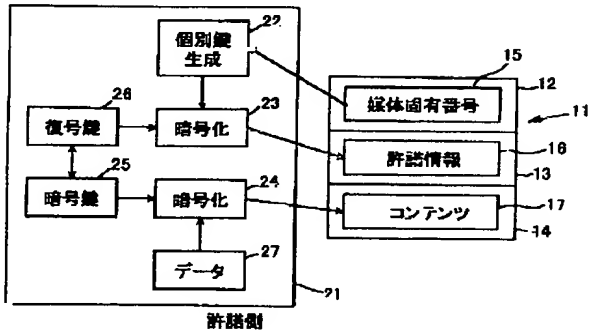
【符号の説明】

１　記録媒体
２　第１階層
３　第２階層
４　第３階層
５　媒体固有番号
６　所定の情報
７　任意の情報
１１　記録媒体
１２　第１階層
１３　第２階層
１４　第３階層
１５　媒体固有番号
１６　許諾情報
１７　コンテンツ
２１　許諾側コンピュータ
２２　個別鍵生成手段
２３　許諾情報暗号化手段
２４　コンテンツ暗号化手段
２５　暗号鍵テーブル
２６　復号鍵テーブル
３１　駆動装置
３２　書込・読出手段
３３　所定情報導出手段
４１　駆動手段
４２　個別鍵生成手段
４３　許諾情報復号化手段
４４　復号鍵格納部
４５　コンテンツ復号化手段
４６　データ格納部
４７　許諾情報暗号化手段
５２　許諾情報更新手段
８３　第２の記録媒体

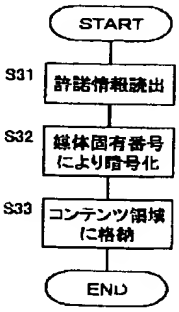
【図１】



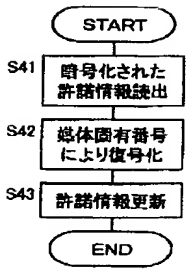
【図２】



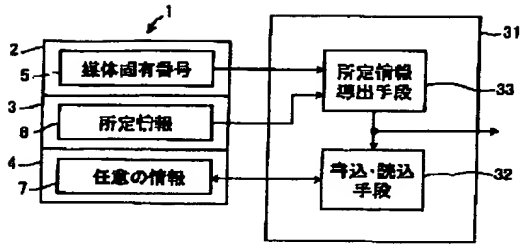
【図７】



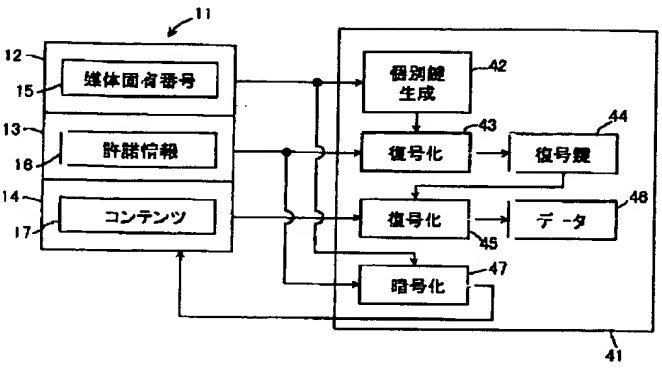
【図９】



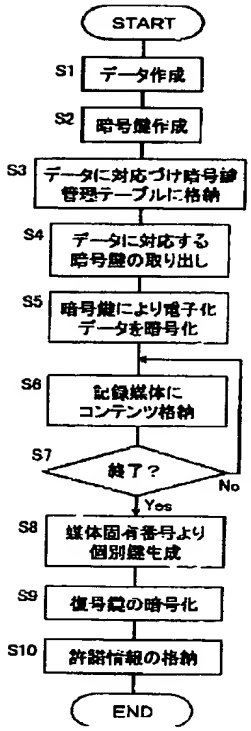
【図3】



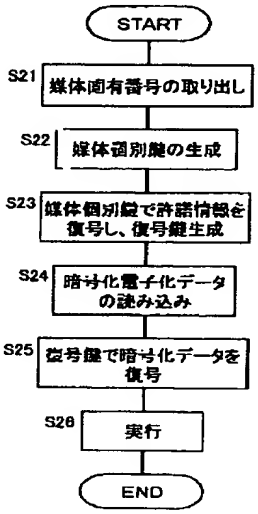
【図4】



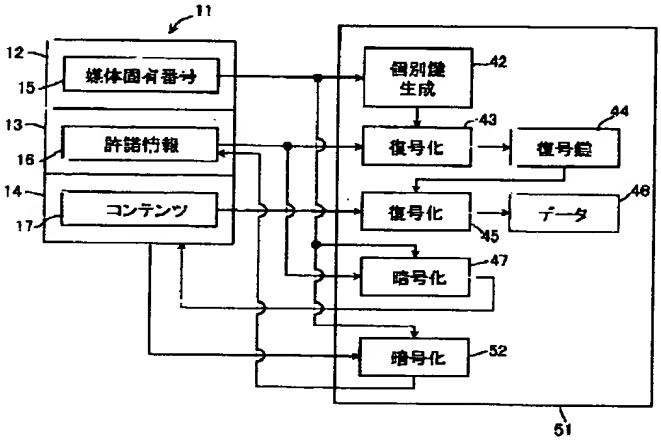
【図5】



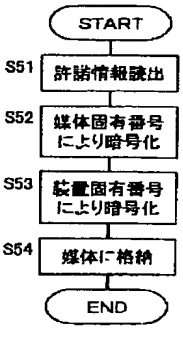
【図6】



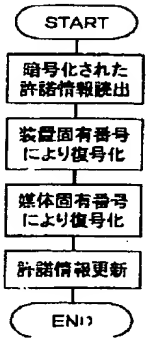
【図8】



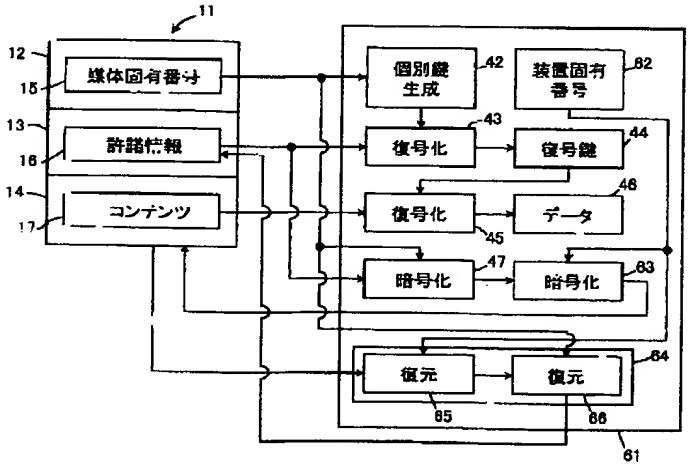
【図11】



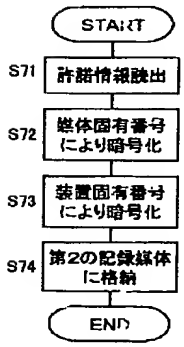
【図12】



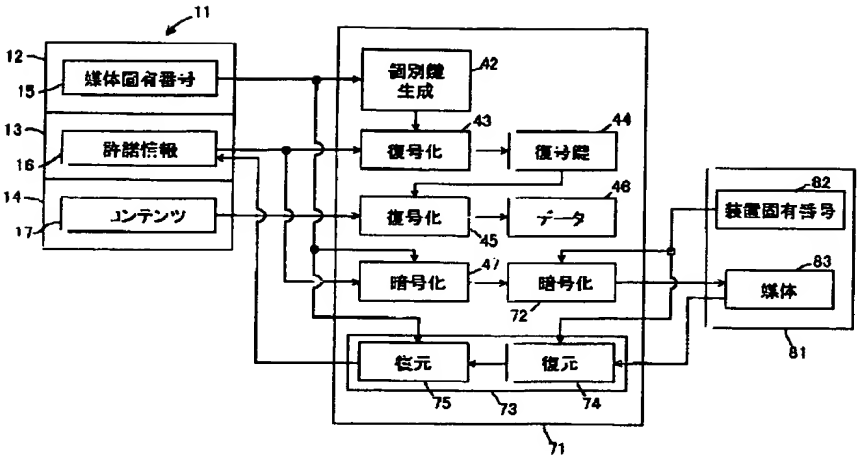
【図10】



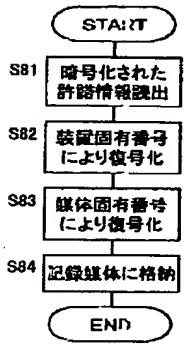
【図14】



【図13】



【図15】



フロントページの続き

(72)発明者　平野　秀幸
神奈川県川崎市中原区上小田中４丁目１番
１号　富士通株式会社内

Ｆターム(参考)　5B017 AA07 BA05 BA07 CA15